Nonadditive Quantum Codes from $\mathbb{Z}_4$-Codes

San Ling
Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University
Block 5 Level 3, 1 Nanyang Walk,
Singapore 637616,
Republic of Singapore
e-mail: lingsan@ntu.edu.sg

Patrick Solé
CNRS-I3S,
Les Algorithmes- bt. Euclide B,
BP.121
2000, route des lucioles,
06 903 Sophia Antipolis,
France.
e-mail: sole@i3s.unice.fr

***Abstract*— Non additive binary quantum codes are constructed by using classical $\mathbb{Z}_4$-linear binary codes.**

I. Introduction

The first quantum codes, the so called stabilizer codes were constructed by using linear quaternary codes [3]. Non additive quantum codes were constructed later in [2], [10] by using union of linear codes or permutation group action [9]. In the present work, we construct binary non additive quantum codes from binary $\mathbb{Z}_4$-linear codes. The argument is based on a description of quantum codes in terms of orthogonal arrays combined with Delsarte celebrated theorem on the equivalence of unrestricted (viz not necessarily linear) codes with given dual distance and orthogonal arrays of given strength [5].

II. Construction

The following characterization of quantum codes was given in [7]:

Theorem II.1. *There exists a quantum $((n, K, d))_q$-code with $K \geq 2$ if and only if there exist K nonzero mappings $\phi_i : \mathbb{F}_q^n \to \mathbb{C}$ $(1 \leq i \leq K)$ satisfying the following condition:*

> *for each partition $\{1, 2, \ldots, n\} = A \cup B$ with $|A| = d-1$ and $|B| = n-d+1$, and any $\mathbf{c}_A$, $\mathbf{c}'_A \in \mathbb{F}_q^{d-1}$, $1 \leq i, j \leq n$,*
>
> $$\sum_{\mathbf{c}_B \in \mathbb{F}_q^{n-d+1}} \overline{\phi_i(\mathbf{c}_A, \mathbf{c}_B)} \phi_j(\mathbf{c}'_A, \mathbf{c}_B) = \delta_{i,j} f$$
>
> *where f is independent of i and depends only on $\mathbf{c}_A$ and $\mathbf{c}'_A$ and δ is Kronecker's symbol.*

Instead of [7, Lemma 2.3, Proposition 2.4 and Corollary 2.5], in order to use $\mathbb{Z}_4$-linear codes for our construction, we use the following analogous results:

Lemma II.2. *Let C be a linear $\mathbb{Z}_4$-code of length n and type $4^{k_1}2^{k_2}$, such that the minimum Lee distance $d(C^\perp)$ of the dual code is at least d. Then for each partition $\{1, 2, \ldots, 2n\} = A \cup B$ with $|A| = d-1$ and $|B| = 2n-d+1$, and any $\mathbf{c}_A \in \mathbb{F}_2^{d-1}$ and $\mathbf{v} \in \mathbb{F}_2^{2n}$, one has*

$$\#\{\mathbf{c}_B \in \mathbb{F}_2^{2n-d+1} \ : \ (\mathbf{c}_A, \mathbf{c}_B) \in \mathbf{v}+C\} = 2^{2k_1+k_2-d+1}.$$

Proof. The Gray image of C is a binary code (not necessarily linear) of length $2n$ and size $2^{2k_1+k_2}$, whose formal dual distance is $d(C^\perp)$. By the equivalence between codes and orthogonal arrays [5], any translate of this Gray image is an orthogonal array of level 2 and strength $d-1$. □

Proposition II.3. *Let C be a linear $\mathbb{Z}_4$-code of length n and $V = \{\mathbf{v}_i\}_{i=1}^K$ be a set of K distinct vectors in $\mathbb{Z}_4^n$. Put*

$$d_v := \min\{w_L(\mathbf{v}_i - \mathbf{v}_j + \mathbf{c}) \ : \ 1 \leq i \neq j \leq K \text{ and } \mathbf{c} \in C\}$$

and $d = \min\{d_v, d(C^\perp)\}$, where w_L denotes the Lee weight. If $d > 0$, then the Gray image of $\bigcup_{i=1}^K (\mathbf{v}_i + C)$ is a binary $((n, K, d))$-quantum code.

Proof. For each $1 \leq i \leq K$, define a mapping $\phi_i : \mathbb{F}_2^{2n} \to \mathbb{C}$ given by

$$\mathbf{u} \mapsto \begin{cases} 1 & \text{if } \mathbf{u} \in \phi(\mathbf{v}_i + C) \\ 0 & \text{if } \mathbf{u} \notin \phi(\mathbf{v}_i + C). \end{cases}$$

It is necessary to verify that the condition in Theorem II.1 is satisfied. For each partition $\{1, 2, \ldots, 2n\} = A \cup B$ with $|A| = d-1$ and $|B| = 2n-d+1$, and any $\mathbf{c}_A, \mathbf{c}'_A \in \mathbb{F}_2^{d-1}$,

$$\overline{\phi_i(\mathbf{c}_A, \mathbf{c}_B)} \phi_i(\mathbf{c}'_A, \mathbf{c}_B) \neq 0$$

if and only if

$$\phi_i(\mathbf{c}_A, \mathbf{c}_B) = \phi_i(\mathbf{c}'_A, \mathbf{c}_B) = 1,$$

i.e., $(\mathbf{c}_A, \mathbf{c}_B), (\mathbf{c}'_A, \mathbf{c}_B) \in \phi(\mathbf{v}_i + C)$. This is equivalent to

$$\phi^{-1}(\mathbf{c}_A, \mathbf{c}_B), \phi^{-1}(\mathbf{c}'_A, \mathbf{c}_B) \in \mathbf{v}_i + C, \qquad \text{(II.1)}$$

which is in turn equivalent to

$$\begin{array}{l} \phi^{-1}(\mathbf{c}_A, \mathbf{c}_B) \in \mathbf{v}_i + C \\ \text{and} \\ \phi^{-1}(\mathbf{c}_A, \mathbf{c}_B) - \phi^{-1}(\mathbf{c}'_A, \mathbf{c}_B) \\ = \phi^{-1}(\mathbf{c}_A, \mathbf{0}) - \phi^{-1}(\mathbf{c}'_A, \mathbf{0}) \in C. \end{array} \tag{II.2}$$

By Lemma II.2 and (II.2), it follows that

$$\begin{array}{l} \sum_{\mathbf{c}_B \in \mathbb{F}_2^{2n-d+1}} \overline{\phi_i(\mathbf{c}_A, \mathbf{c}_B)} \phi_i(\mathbf{c}'_A, \mathbf{c}_B) \\ = \begin{cases} 0 & \text{if } \phi^{-1}(\mathbf{c}_A, \mathbf{0}) - \phi^{-1}(\mathbf{c}'_A, \mathbf{0}) \notin C \\ 2^{2k_1+k_2-d+1} & \text{if } \phi^{-1}(\mathbf{c}_A, \mathbf{0}) - \phi^{-1}(\mathbf{c}'_A, \mathbf{0}) \in C. \end{cases} \end{array}$$

If $1 \leq i \neq j \leq K$, since $w_L(\phi^{-1}(\mathbf{c}_A, \mathbf{0}) - \phi^{-1}(\mathbf{c}'_A, \mathbf{0})) = w_H(\mathbf{c}_A - \mathbf{c}'_A, \mathbf{0}) \leq d-1 < d \leq w_L(\mathbf{v}_i - \mathbf{v}_j + C)$, it follows that $\phi^{-1}(\mathbf{c}_A, \mathbf{0}) - \phi^{-1}(\mathbf{c}'_A, \mathbf{0}) \notin \mathbf{v}_i - \mathbf{v}_j + C$. Hence, $\overline{\phi_i(\mathbf{c}_A, \mathbf{c}_B)} \phi_j(\mathbf{c}'_A, \mathbf{c}_B) = 0$ for all $\mathbf{c}_B$, which therefore implies

$$\sum_{\mathbf{c}_B \in \mathbb{F}_2^{2n-d+1}} \overline{\phi_i(\mathbf{c}_A, \mathbf{c}_B)} \phi_j(\mathbf{c}'_A, \mathbf{c}_B) = 0.$$

□

Corollary II.4. *Suppose C, C' are two linear $\mathbb{Z}_4$-codes of length n such that $C \subseteq C'$, with $|C| = 4^{k_1} 2^{k_2}$ and $|C'| = 4^{k'_1} 2^{k'_2}$. Then there exists a binary $((2n, K, d))$-quantum code with $K = 2^{2k_1+k_2-2k'_1-k'_2}$ and $d = \min\{d(C' \setminus C), d(C^\perp)\}$.*

Proof. With notation as in Proposition II.3, take V to be a set of coset representatives of the K distinct cosets of C in C'. This corollary then follows immediately from Proposition II.3. □

III. Examples

In this section, we illustrate the above construction with several well-known linear $\mathbb{Z}_4$-codes.

Example III.1. *Let C be the linear $\mathbb{Z}_4$-code of length 2^m, size 4^{m+1} and minimum Lee distance $2^m - 2^{\frac{m-1}{2}}$ (m odd) whose binary Gray image is a Kerdock code. The dual code $C^\perp$ has size 4^{2^m-m-1} and minimum Lee distance 6, and its Gray image is a binary Preparata-like code. It is well known that $C \subset C^\perp$. By Corollary II.4, we obtain a family of binary $((2^{m+1}, 2^{2^{m+1}-4m-4}, 6))$-quantum codes, for m odd. The parameters of this family are slightly inferior to the quantum codes of parameters $((2^m, 2^{2^m-3m-2}, 6))$ in [1].*

Example III.2. *Let C be the linear $\mathbb{Z}_4$-code of length 2^m, size $4^{m+1}2^{rm}$ and minimum Lee distance $2^m - 2^{r+\frac{m-1}{2}}$ (m odd and $1 \leq r \leq m-1/2$) whose binary Gray image is a Delsarte-Goethals code. The dual code $C^\perp$ has size $2^{2^{m+1}-2m-2-rm}$ and minimum Lee distance 8 when $r \geq 3$, and its Gray image is a binary Goethals-Delsarte code. Since $C \subseteq QRM(2,m)$, where $QRM(2,m)$ is the quaternary Reed-Muller code which is known to be self-orthogonal, it follows that $C \subseteq C^\perp$. By Corollary II.4, we obtain a family of binary $((2^{m+1}, 2^{2^{m+1}-4m-2rm-4}, 8))$-quantum codes, for m odd. When $r=3$, the parameters of some of the first examples obtained are: for $m=7$, $((256, 2^{182}, 8))$; for $m=9$, $((1024, 2^{930}, 8))$.*

Example III.3. *Taking in Corollary II.4 in the notation of [4], $C = D_4^\perp$ and for C' the Calderbank McGuire code in length 32 over $\mathbb{Z}_4$ yields a $((64, 2^{10}, 12))$, which is as good as the best-known quantum binary code [8].*

References

[1] J. Bierbrauer and Y. Edel, Quantum twisted codes, J. Comb. Des., vol. 8, no. 3, 174 – 188 (2000)

[2] M. Grassl and Thomas Beth, A Note on Non-Additive Quantum Codes,1997, preprint `quant-ph/9703016v1`

[3] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction via codes over $\mathrm{GF}(4)$.IEEE Trans. Information Theory, 44 (1998), pp. 1369-1387.

[4] Calderbank, A. R.; McGuire, Gary M. Construction of a $(64, 2^{37}, 12)$ code via Galois rings. Des. Codes Cryptogr. 10 (1997), no. 2, 157–165.

[5] Delsarte, Philippe, Four fundamental parameters of a code and their combinatorial significance. Information and Control 23 (1973), 407–438.

[6] Hammons, A. Roger, Jr.; Kumar, P. Vijay; Calderbank, A. R.; Sloane, N. J. A.; Solé, Patrick The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. IEEE Trans. Inform. Theory 40 (1994), no. 2, 301–319.

[7] K. Feng, S. Ling & C. Xing, Asymptotic bounds on quantum codes from algebraic geometry codes, *IEEE Trans. Inform. Theory* **52**, no. 3 (2006), 986 – 991

[8] Markus Grassl, QECC section of `http://www.codetables.de/`

[9] Harriet Pollatsek, Mary Beth Ruskai, Permutationally invariant codes for quantum error correction, Linear Algebra and its Applications 392 (2004) 255-288

[10] R. M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane, "A Nonadditive Quantum Code", Phys. Rev. Letters, 79 (1997), pp. 953-954.M